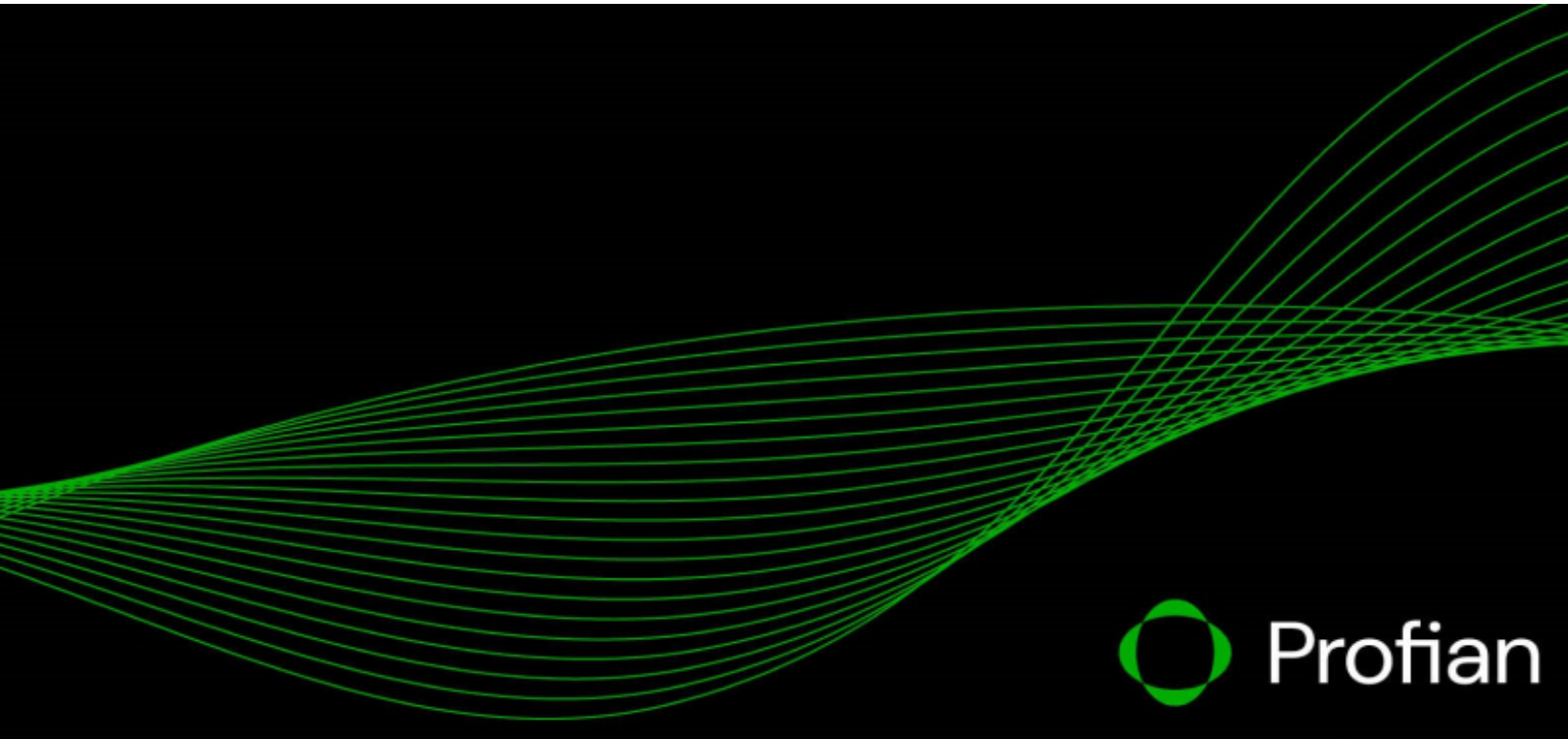
Profian

WHAT IS CONFIDENTIAL COMPUTING?

Learn about TEEs, attestation, and Profian Assure.



Profian

"Confidential Computing is the protection of data in use by performing computation in a hardware-based Trusted Execution Environment" as defined by the Confidential Computing Consortium[1].

Confidential Computing, or encrypting *data in use* within a secure hardware environment, completes the data security triangle since data at rest (in storage) and in transit (across networks) are routinely encrypted.

What is a TEE?

Today's modern data centers are built on the latest hardware which provide isolated areas – think built-in "mini-vaults" – inside each CPU. These vaults are called Trusted Execution Environments (TEEs) and they allow for hardware-based encryption of data in use. Taking advantage of TEEs to protect and encrypt data in use is the cutting-edge security technology known as Confidential Computing.

Examples of hardware-based Trusted Execution Environments (TEEs) include Intel® SGX and AMDI® SEV technologies, which provide chip-based capabilities to allow the creation of applications that are protected from the host computer, including its administrators[2], allowing the protection of both the data they are processing and the applications themselves. These approaches address the problem inherent in existing cloud computing technologies by restricting access to the applications running on a host to the CPU only, blocking all other access by applications or users of the system.

[1] Confidential Computing Consortium, 2021, A Technical Analysis of Confidential Computing, v1.2, https://confidentialcomputing.io/wp-content/uploads/sites/85/2022/01/CCC-A-Technical-Analysis-of-Confidential-Computing-v1.2.pdf

[2] Note that the AWS Nitro Enclaves® service does not meet this definition, as it does not provide sufficient protection from administrators and operators of the system to ensure that they cannot access data or applications.

TEE instances allow organizations to protect their applications and data in use, but there is one important step that must be taken before it is safe to deploy applications into TEEs: attestation. It is vital to ensure that a TEE instance has both been correctly set up and is also not the result of a malicious actor pretending to have set one up. Attestation is the process that allows this to take place.

What is attestation?

Once a TEE instance has been set up, it is possible to request that the CPU chip[3] that created it produces a cryptographic measurement of the memory the instance contains. This measurement is then cryptographically signed by the chip, and can be sent to an attestation service which checks that the measurement is correct (against a set of expected values) and that the entity which performed the measurement and signing is a real chip from a trusted vendor, with the expected capabilities.

If this validation check fails, the TEE instance should not be used, and the application should not be deployed to it.

Because the measurement is performed by the chip, and not the operating system, this attestation process allows the assurance that there is no opportunity for a malicious or compromised host to "spoof" a TEE instance. As long as the attestation is properly validated, this means there is a cryptographic proof that the Cloud Service Provider cannot interfere with the application. This validation must, however, be performed by an independent trusted party: in order to allow a true trust relationship to the TEE instance to be established, the entity providing the attestation must not be associated with the Cloud Service Provider.

If the entity performing the attestation is associated with the owner or operator of the systems running the TEE instances, it would be easy for

[3] The process involves the chip and its associated firmware, which are cryptographically linked.

them to provide false assertions that attestation was successful, all-the-while spoofing the TEE instance: there is no way for the organization deploying the application to know.

For a deeper understanding of TEEs and attestation, download our white paper.

Secure existing workloads with Profian Assure

Profian's flagship Confidential Computing solution, Profian Assure, makes it easy to create encrypted, private environments on public cloud hardware to protect both data and applications while in use.

Profian Assure provides an added layer of security to your Confidential Computing environment through an automatic attestation process, which restricts the deployment of your workload to the secure environment until the attestation process is complete. Receive neutral, third-party validation that your "virtual vault" has been created properly to protect both your applications and data before they are deployed.

Rely on Profian Assure's attestation certificates to satisfy regulators, stay in compliance and build trust with your customers.

Profian

Profian delivers Confidential Computing solutions that solve for security of data in use, a well-known vulnerability of cloud computing. We help security teams seamlessly create private environments on public cloud hardware so organizations can enjoy the speed, scale and cost-saving benefits of cloud computing for even the most sensitive workloads. Profian's third-party attestation service helps meet regulatory standards and build trust with customers. Our solution builds on the open source project Enarx, of which Profian is the custodian.

Profian is a a member of the following organizations: